



**ATTENTION:** Users of IATA Products and Services –  
Administrative services responsible for settling  
invoices

**SUMMARY:** Recent attempts have been made through fraudulent e-mail messages to obtain payments from users of IATA products and services. The purpose of this **SECURITY ALERT** is to:

- Inform you on the actions taken by IATA;
- Provide information to help you detect similar attempts;
- Provide guidelines on reporting to IATA of any such attempts that you detect.

We have implemented steps to assist you in verifying the authenticity of every e-mail that you receive from IATA. These are also described below.

**ACTION:** Please read the information below and share it with colleagues in your company's administrative services who are responsible for settling IATA invoices.

If you have any questions concerning this security alert, kindly e-mail your queries to [information.security@iata.org](mailto:information.security@iata.org).

Thank you for your attention on this matter.

**Ayaz M. Hussain**  
Senior Vice President & Chief Financial Officer  
IATA

**SECURITY ALERT      SECURITY ALERT      SECURITY ALERT**

**I. GENERAL DESCRIPTION OF TACTICS USED BY FRAUDSTERS**

Fraudulent e-mails seeking payment have been received by users of IATA products and services.

The methods employed generally include elements of the following:

- i. the fraudster contacts users under a false name, sometimes similar or identical to the names of IATA officials, seeking payment for products or services and/or claiming payments for outstanding amounts due;



- ii. the fraudster uses an e-mail address resembling IATA e-mail addresses but using different host servers such as “gmail”;
- iii. the fraudster uses a technique which allows the name of the sender of an e-mail to be doctored and masked, so that the e-mail appears to have been sent from a valid IATA address;
- iv. the fraudster e-mails forged documents bearing the official IATA logo, most likely copied from our website.

## **II. COUNTER-MEASURES TAKEN BY IATA**

IATA has taken a number of steps in response to such attempts that have been notified to us. Our actions include initiation of investigation by the police and relevant authorities in the applicable jurisdictions, as well as communication with banks hosting the fraudulent bank accounts and requesting their cooperation in investigating suspected frauds.

Specific actions for your attention are listed below:

- 1) All bona fide IATA e-mails use the "[@iata.org](mailto:@iata.org)" domain. It is the only domain permitted for the purpose of conducting IATA business.
- 2) Every out-going email from "[@iata.org](mailto:@iata.org)" has a digital signature with a certificate issued by GlobalSign, a “trusted certificate authority”. You can use the digital signature to verify the authenticity of the e-mail and that it is from IATA.
- 3) Accordingly, every bona fide payment request or reminder that is sent by IATA through e-mail will be transmitted using the domain “[@iata.org](mailto:@iata.org)” and will carry a digital signature. For guidelines on how to use the digital signature to verify the authenticity of the sender, please click [here](#).

## **III. WHAT YOU CAN DO TO PROTECT YOUR ORGANIZATION**

### **1. Recognizing Fraudulent E-mails**

Being able to recognize such e-mails can help prevent you from becoming a victim. Here are [examples](#) of some recent e-mails received by users of IATA products and services.

### **2. Reporting Fraudulent E-mails**

If you receive a suspicious or potentially fraudulent e-mail, please report the relevant information to the following e-mail address: [information.security@iata.org](mailto:information.security@iata.org).



When reporting such messages, it is important to copy and paste the entire e-mail, including the header information.

To display full message headers: Open the mail message.

*In Outlook 2007:* double-click the message so that it opens in its own window. In the Options group, click the dialog box launcher (small square with an arrow).

*In Outlook 2003:* from the View menu, select Options. The message headers are at the bottom of the window, in a box labeled "Headers:" or "Internet headers:"

To insert the headers into an e-mail message: Select all the headers by clicking and dragging the cursor from the top left corner to the bottom right corner of the header text. Press Ctrl-c to copy the headers to the Clipboard. Create a new e-mail message, click in its main text window, and press Ctrl-v to paste the headers. Transmit the e-mail to [information.security@iata.org](mailto:information.security@iata.org)

If you believe you are a victim of e-mail fraud attempt, we recommend that you also contact your local law enforcement authority immediately.

### **3. Recognizing Authentic IATA E-mails**

The items below illustrate some of the e-mail components that will help you identify an authentic message coming from IATA.

- i. All authentic IATA emails use "[@iata.org](mailto:information.security@iata.org)" addresses ONLY.
- ii. All authentic IATA emails contain a digital signature with certificates issued by GlobalSign.
- iii. If your email system can handle S/MIME you can view the certificate by clicking on the digital signature and then view details/view certificate.

For guidelines on how to use the digital signature and verify the authenticity of the sender, please click [here](#).



#### **4. IATA Invoices and Payment Reminders**

All authentic IATA Invoices are on IATA letterhead and specify either an IATA bank account into which the settlement payment must be made or specify that the settlement must be through the IATA Clearing House.

As of July 19, 2010 all authentic payment requests or reminders from IATA are either through an e-mail with a Digital Signature attached to verify the authenticity of the sender, or through a letter on an IATA letterhead.

An authentic IATA Invoice or an IATA payment reminder will **never** request settlement payment into a non-IATA bank account.